Unteranlage zur Datenverarbeitungsvereinbarung – Spezifizierung der Verarbeitung personenbezogener Daten

1. KONTAKTINFORMATIONEN

	PI/URKUND	Der Kunde
Name und Firmenregistrierungsnummer	Prio Infocenter AB 556483-9032	
Vertreter	Andreas Ohlson, CEO	
Ansprechpartner für Fragen zur DSGVO	Peter Witasp, +468-7385200, dataprotection@urkund.com	

2. ANWEISUNGEN

2.1 Kurzbeschreibung der Dienstleistungen im Rahmen der Vereinbarung sowie der Zwecke der Verarbeitung

PI/URKUND verarbeitet personenbezogene Daten, um zu überprüfen, ob die eingereichten Texte Ähnlichkeiten mit anderen Quellen aufweisen, was darauf hindeuten könnte, dass der Text ganz oder teilweise plagiiert wurde. Personenbezogene Daten der Studierenden werden von PI/URKUND gespeichert, um sie der Lehrkraft, die den entsprechenden Text eingereicht hat, anzeigen zu können. Personenbezogene Daten von Lehrkräften und Administratoren werden von PI/URKUND gespeichert, um die Registrierung und Pflege von Benutzerkonten zu ermöglichen. Personenbezogene Daten von Kunden werden von PI/URKUND gespeichert, um Vereinbarungen über die Dienstleistungen von PI/URKUND eingehen zu können.

2.2 Kategorien von personenbezogenen Daten

- E-Mail-Adressen
- Sprachlicher Stil
- IP-Adresse
- Schibboleth-Identität
- Name
- Dokumente (die im Fließtext personenbezogene Daten enthalten können)
- E-Mail-Nachrichten (die im Hauptteil der Nachricht personenbezogene Daten enthalten können)
- Anmerkungen zur Einreichung (die im Text personenbezogene Daten enthalten können)

PI/URKUND verarbeitet keine sensiblen personenbezogenen Daten wie z. B. ethnische Herkunft, sexuelle Orientierung, religiöse Überzeugungen, gesundheitliche Entwicklung usw. Wenn sich herausstellt, dass Daten dieser Kategorie im Textkörper des Dokuments an PI/URKUND gesendet wurden, ist der Datenverantwortliche für die sofortige Löschung oder Maskierung der Daten oder die Anonymisierung der personenbezogenen Daten, mit denen sie möglicherweise verknüpft sind, verantwortlich.

Kommt der Datenverantwortliche zu dem Schluss, dass personenbezogene Daten sensibler Art an URKUND übermittelt werden, so ist er dafür verantwortlich, PI/URKUND im Voraus Anweisungen über den Umgang mit diesen Dokumentdaten zu übermitteln.

2.3 Kategorien von betroffenen Personen

PI/URKUND registriert personenbezogene Daten von Kunden, Ansprechpartnern, Administratoren, Lehrkräften und Studierenden.

2.4 Verarbeitungsaktivitäten (Speicherung, Verwaltung, datenbankübergreifende Abfragen usw.)

PI/URKUND registriert/speichert und verarbeitet personenbezogene Daten, die PI/URKUND zum Zwecke der Durchführung von Plagiatkontrollen gemäß Dienstleistungsvereinbarungen und zur Information von Kunden und Nutzern über Neuigkeiten und Informationen, die für Kunden/Nutzer von Interesse sein können, erhält. Im Rahmen der Verarbeitung werden in den gespeicherten Dokumenten Suchen durchgeführt, um Ähnlichkeiten mit den eingereichten Dokumenten zu finden. Diese werden anschließend bearbeitet und die festgestellten Ähnlichkeiten werden in einer Webschnittstelle angezeigt, auf die Benutzer mit einer gültigen Vereinbarung mit PI/URKUND Zugriff haben. Ein Link zu diesem Dokument befindet sich in dem Bericht und kann, sofern keine gesonderte Vereinbarung getroffen wurde, zum detaillierten Vergleich der Werke heruntergeladen werden. Aus den Nutzungsbedingungen von URKUND geht eindeutig hervor, dass der Nutzer die zur Verfügung gestellten Informationen ausschließlich zum Zwecke der Überprüfung des Vorliegens eines Plagiats verwenden darf.

2.5 Standort für die Verarbeitung personenbezogener Daten

PI/URKUND führt die gesamte Verarbeitung personenbezogener Daten auf Servern durch, die sich physisch in Schweden befinden.

3. SICHERHEITSVORKEHRUNGEN

PI/URKUND nimmt zum Schutz personenbezogener Daten kontinuierlich Verbesserungen an der technischen Umgebung vor und hat darüber hinaus organisatorische und technische Sicherheitsvorkehrungen getroffen, um den Zugang des Personals zu personenbezogenen Daten zu begrenzen.

PI/URKUND beachtet den Schutz der Privatsphäre, indem es den Zugang zu Informationen für Personal, das Zugang zu personenbezogenen Daten hat, einschränkt, und indem es sicherstellt, dass das Personal nur Benutzerkonten und Berechtigungen erhält, die auf den Erfordernissen seiner Arbeitsaufgaben basieren.

PI/URKUND stellt sicher, dass bei der Verarbeitung personenbezogener Daten ein angemessenes Sicherheitsniveau aufrechterhalten wird. Dies umfasst sowohl organisatorische als auch technische Sicherheitsvorkehrungen. Die Sicherheitsarbeit bei PI/URKUND muss in Form eines fortlaufenden Prozesses mit Zustimmung der Geschäftsleitung erfolgen. Jegliche Verstöße müssen unverzüglich gemeldet und behoben werden, und die daraus gezogenen Lehren müssen anschließend zur Verhinderung künftiger Verstöße genutzt werden. Penetrationstests müssen regelmäßig, mindestens alle

zwei Jahre, durchgeführt werden. Dringende Entdeckungen in Verbindung mit derartigen Tests müssen nach Priorität geordnet und umgehend behandelt werden.

Alle anderen Sicherheitsmaßnahmen, die zwischen PI/URKUND und dem Kunden vereinbart wurden, müssen dokumentiert und von beiden Parteien unterzeichnet werden.

3.1.1 Regeln zum Speichern/Löschen

Während der Laufzeit der Vereinbarung: So schnell wie möglich und spätestens innerhalb von 30 Tagen ab dem Zeitpunkt, an dem der Kunde die Löschung der personenbezogenen Daten beantragt hat.

Um laufende Disziplinarverfahren nicht zu beeinträchtigen oder zu erschweren, anonymisiert oder löscht PI/URKUND personenbezogene Daten nur auf Anweisung des Datenverantwortlichen, es sei denn, diese werden vom Kunden über ein von PI/URKUND zur Verfügung gestelltes Tool abgewickelt. Liegen keine Anweisungen des Datenverantwortlichen vor, kann PI/URKUND aus Speicherplatzgründen dennoch bestimmte Daten 25 Monate nach Eingang des Dokuments bei PI/URKUND löschen.

Nach der Beendigung der Vereinbarung: Siehe Abschnitt 9 der Datenverarbeitungsvereinbarung

3.1.2 Sicherheitsbestimmungen

Die gesamte Speicherung und Bearbeitung von personenbezogenen Daten findet in Stockholm statt. Die IT-Umgebung wurde mit einem hohen Maß an Sicherheit sowohl in Bezug auf die physische als auch die logistische Sicherheit eingerichtet. Die IT-Umgebung ist redundant und befindet sich an zwei geografisch getrennten Standorten. Der gesamte Zugang zu den Räumlichkeiten wird durch ein Zutrittssystem, Kameraüberwachung und Firewall-Lösungen geschützt. Die Stromversorgung wird mit Hilfe separater dieselbetriebener Notstromsysteme sichergestellt. Alle Mitarbeiter durchlaufen eine gründliche Sicherheitsschulung, in der die Routinen für den Umgang mit Benutzerkonten/Passwörtern, Virenschutz, das Herunterladen von Software, die Entsorgung von Materialien, die externe Nutzung von Computern usw. vermittelt werden.

Die IT-Sicherheit ist bei unserer Entwicklungsarbeit stets ein wichtiger Faktor und wir testen regelmäßig gegen bekannte Schwachstellen.

Patches von Produktionsservern erfolgen regelmäßig einmal im Monat sowie wenn nötig, wenn z. B. eine ernsthafte Sicherheitslücke in einem Betriebssystem entdeckt wird.

Alle Computer und Server werden mit Hilfe eines Unternehmens physisch vernichtet, das dafür sorgt, dass es nicht möglich ist, Daten nach der Vernichtung wieder herzustellen.

Berechtigungs- und Zugriffskontrollen

Um eine vollständige Rückverfolgbarkeit zu gewährleisten, erfolgt der gesamte Zugriff auf die Verwaltungssysteme über individuell verschlüsselte Passwörter und Benutzerkonten. Der Zugriff erfolgt auf Bedarfsbasis und verschiedene Berechtigungsstufen steuern, auf welche Informationen ein Benutzer zugreifen kann.

Der Zugriff auf die Produktionsumgebung ist denjenigen Technikern bei PI/URKUND oder Unterauftragnehmern vorbehalten, die für die Wartung/Weiterentwicklung des Systems Zugang benötigen, und dieser muss vom „Betriebsleiter“ genehmigt werden, bevor der Zugriff gewährt wird.

Eingabedatenmaterial, das personenbezogene Daten enthält

Das Eingabedatenmaterial wird auf drei verschiedenen Ebenen gespeichert. Protokolldateien (zur Fehlerbehebung und Rückverfolgbarkeit), Datenbanken und Dateisysteme. Wir bemühen uns, lediglich ein Minimum an personenbezogenen Daten zu speichern, und für die Nutzung des Systems ist grundsätzlich eine E-Mail-Adresse erforderlich, die anonymisiert werden kann. Wir empfehlen, in den eingereichten Dokumenten keine personenbezogenen Daten im Fließtext aufzuführen. Wenn dies geschieht, sollte es in einer Form erfolgen, die es schwierig gestaltet, die Identität festzustellen, z. B. eine ID-Nummer, die in einem separaten System gespeichert ist.

Ausgabedatenmaterial, das personenbezogene Daten enthält

Es können Systemeinstellungen verwendet werden, die den Zugriff auf personenbezogene Daten einschränken. Dies kann z. B. bedeuten, dass das Dokument von zukünftigen Suchvorgängen ausgeschlossen wird, dass es automatisch gelöscht wird, und darüber bestimmen, welche Informationen über Absender und Empfänger sowohl innerhalb der Organisation als auch nach außen hin angezeigt werden. Die zu erstellende Konfiguration wird zwischen dem Kunden und PI/URKUND vereinbart. Wo keine gesonderte Vereinbarung getroffen wurde, stimmt der Kunde der Weitergabe von Dokumenten und personenbezogenen Daten an andere Bildungseinrichtungen, die eine gültige Vereinbarung mit PI/URKUND haben, zu, um die Feststellung von plagiierten Materialien zwischen diesen Einrichtungen zu ermöglichen.

Externe Kommunikationsverbindungen

Die gesamte Kommunikation zwischen den Anwendungen und Datenbanken von PI/URKUND erfolgt mit Hilfe von Verschlüsselung (SSL). Eine Ausnahme bilden die Fälle, in denen die Benutzer zum Einreichen der Dokumente E-Mail verwenden.

Die Produktionsumgebung von PI/URKUND ist logistisch durch Firewalls und Netzwerke getrennt, die externe Web-Frontends vom Backend trennen.

Protokollierung

PI/URKUND protokolliert Transaktionen, die in unseren Systemen stattfinden. Die Protokolle werden im Textformat gespeichert und können personenbezogene Daten wie IP-Nummer oder ID-Nummer enthalten. Sie werden in der Regel maximal sechs Monate gespeichert, bevor sie gelöscht werden, sofern nichts anderes vereinbart wurde. Diese Protokolle werden zur Fehlerbehebung sowie zur Untersuchung versuchter Zuwiderhandlungen verwendet.

4. VORAB GENEHMIGTE UNTERBEAUFTRAGTE DATENVERARBEITER

PI/URKUND ist berechtigt, die folgenden Unterauftragnehmer zur Verarbeitung personenbezogener Daten im Rahmen der Datenverarbeitungsvereinbarung einzusetzen:

Name	Zweck	Ort der Verarbeitung (Land)
Teknik i Media Datacenter Stockholm Aktiebolag	Hardware-Anbieter: Netzwerk und Server.	Schweden
H1 Communication AB	Anbieter von Kundenbetreuung	Schweden
Easy Correct ApS	Softwaretechnologie-Anbieter: Feedback-Lösung	Dänemark